Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Currently Amended)   A telecommunications system arranged for providing Single Sign-On (SSO) services for a user roaming with a user equipment (UE) in a packet radio network of a Multinational Mobile Network Operator (MN-MNO) that includes a federation of National Network Operators (NNO), one of these National Network Operators holding the user's subscription, the telecommunications system comprising:

a visited Gateway GPRS Support Node (V-GGSN) assigned for the user at a visited packet radio network wherein the user is roaming, the V-GGSN sending user's identifiers relevant for the user's authentication toward the user's home network; ~~and~~

a home Authentication, Authorization and Accounting (H-AAA) server in the user's home service network, responsible for maintaining a master session for the user with said user's identifiers;

a visited Authentication, Authorization and Accounting (V-AAA) server ~~(13)~~ in the visited network, acting as a proxy between the V-GGSN and the H-AAA, and binding an H-AAA address with said user's identifiers; ~~and~~

a global Single Sign-On Front End (G-SSO-FE) utilized as a single entry point for Single Sign-On service in the Multinational Mobile Network Operator federation;~~[[,]]~~ ~~each service provider in the federation providing a specific Uniform Resource Identifier~~ ~~(URI) as a physical SSO entry point towards the federation;~~ and

<u>a number of Service Providers that have signed service agreements with the Multinational Mobile Network Operator federation for offering Single Sign-On services to users that are subscribers of any National Network Operator included in the federation, each Service Provider in the federation providing a specific Uniform Resource Identifier (URI), as physical SSO entry point towards the federation, and each Service Provider comprising:</u>

redirection means for redirecting the user to the global Single Sign-On Front End (G-SSO-FE) as entry point in the federation;

receiving means for receiving a token from the user along with an indication of where the token was generated;

retrieval means for retrieving an authentication assertion from a site where the token was generated; and

checking means for checking that such site is trusted.

2.   (Previously Presented)   The telecommunications system of claim 1, further comprising a Global Directory of the Multinational Mobile Network Operator federation cooperating with the visited Authentication, Authorization and Accounting server in the visited network wherein the user is roaming to locate the home Authentication, Authorization and Accounting server in the user's home service network.

3.   (Previously Presented)   The telecommunications system of claim 2, wherein the Global Directory is an entity arranged for storing an association between user's identifiers relevant for user's authentication and an address of a corresponding home Authentication, Authorization and Accounting server.

4.   (Previously Presented)   The telecommunications system of claim 1, wherein the visited Authentication, Authorization and Accounting server in the visited network wherein the user is roaming, keeps a binding of a home Authentication, Authorization and Accounting server address and user's identifiers within a Local Dynamic Routing Database.

5.   (Previously Presented)   The telecommunications system of claim 4, wherein said user's identifiers comprise a user directory number and an IP address assigned to the user.

6.   (Previously Presented)   The telecommunications system of claim 1, wherein the home Authentication, Authorization and Accounting server in the user's home service network maintains a master session for the user in cooperation with a Single Sign-On Session Database (SSO Session DB) for storing session related information comprising a user directory number, an IP address assigned to the user, an indicator of a selected authentication mechanism, and a timestamp.

7.   (Currently Amended)   The telecommunications system of claim 1, <u>wherein the token is either an authentication assertion or a reference thereof.</u> ~~further comprising a number of Service Providers that have signed service agreements with the Multinational Mobile Network Operator federation for offering Single Sign-On services to users that are subscribers of any National Network Operator included in the federation, each Service Provider comprising:~~

~~redirection means for redirecting a user to the global Single Sign-On Front End (G-SSO-FE) as entry point in the federation;~~

~~receiving means for receiving a token from the user, the token being either an authentication assertion, or a reference thereof along with an indication of where such assertion was generated;~~

~~retrieval means for retrieving an assertion from a site where the assertion was generated ; and~~

~~checking means for checking that such site is trusted.~~

8.   (Currently Amended)   The telecommunications system of claim <u>1</u> [[7]], wherein each particular Service Provider may have a different global Single Sign-On Front End for acting as entry point in the federation.

9.   (Previously Presented)   The telecommunications system of claim 8, wherein each particular Service Provider further comprises means for changing from one global Single Sign-On Front End to another within the federation for acting as entry point in said federation.

10.   (Currently Amended)   A method for providing Single Sign-On services through a number of Service Providers having service agreements with a Multinational Mobile Network Operator (MN-MNO) for a user roaming with a user equipment (UE) in a packet radio network of said Multinational Mobile Network Operator that includes a federation of National Network Operators, one of these National Network Operators being a home service network for the user and holding the user's subscription, the method comprising the steps of:

(a) authenticating the user roaming in a visited packet radio network, via a proxy, toward the user's home service network; and

(b) creating a master session at the user's home service network with Single Sign-On related data;

(c) redirecting the user accessing a Service Provider, that has a service agreement with the Multinational Mobile Network Operator, toward the user's home network via a global Single Sign-On Front End (G-SSO-FE) entry point in the federation for obtaining a Single Sign-On authentication assertion, each service provider in the federation providing a specific Uniform Resource Identifier as a Single Sign-On service; and

(d) receiving a Single Sign-On authentication assertion either from the user or from an entity where such assertion was generated, along with an address of such entity; and

(e) validating the Single Sign-On authentication assertion with the entity having generated the assertion.

.

11.   (Previously Presented)   The method of claim 10, wherein the step b) of creating a master session at the user's home service network with Single Sign-On related data further comprises the steps of:

storing at a Single Sign-On Session Database Single Sign-On related data comprising a session identifier, a session status, a user directory number, an IP address

assigned to the user, an indicator of a selected authentication mechanism, and a timestamp of the authentication event; and

binding at a user's visited service network an address of an entity handling the master session for such user at the user's home service network, and a set of user's identifiers that includes at least a user directory number, and an IP address assigned to the user.

12.   (Previously Presented)   The method of claim 10, wherein the step a) of performing a first authentication of a user roaming in a visited packet radio network includes a step of assigning a visited Gateway GPRS Support Node for the user at the visited packet radio network.

13.   (Previously Presented)   The method of claim 12, wherein the step of assigning a visited Gateway GPRS Support Node includes a step of sending user's identifiers relevant for a first user's authentication from said visited Gateway GPRS Support Node toward a home Authentication, Authorization and Accounting server in the user's home service network for maintaining a user's master session.

14.   (Previously Presented)   The method of claim 13, wherein the step of sending user's identifiers includes a step of interposing a visited Authentication, Authorization and Accounting server in the visited network, acting as a proxy between said visited Gateway GPRS Support Node and the home Authentication, Authorization and Accounting server in user's home network.

15.   (Previously Presented)   The method of claim 10, wherein the step c) of redirecting a user toward the user's home network via a global Single Sign-On Front End (G-SSO-FE) comprises the steps of:

c1) determining a visited network which assigned the current IP address to the user when accessing the federation network; and

c2) obtaining from the visited network an address of an entity handling a user's master session in the user's home service network.

16.   (Previously Presented)   The method of claim 15, wherein the step c2) of obtaining an address of an entity handling the master session for such user includes a step of redirecting the user toward the currently visited network.

17.   (Previously Presented)   The method of claim 15, wherein the step c2) of obtaining an address of an entity handling the master session for such user includes a step of requesting such address from the global Single Sign-On Front End toward the visited network by using a Back-End protocol.

18.   (Previously Presented)   The method of claim 15, wherein the step c1) of determining the visited network includes a step of querying a Global Directory about the National Network Operator in charge of assigning a given user's IP address.

19.   (Currently Amended)   The method of claim 10, wherein the step d) of receiving a Single Sign-On authentication assertion from the entity where such assertion was generated includes a step of: the steps of:
        receiving from the user a reference to said assertion along with an address of such entity.
        ; and
        validating the assertion with the entity having generated the assertion.